GOTS Utilities for Windows NT Security and CM Enhancement

NTAG Overview Presentation

15 January 1998

Mr. Charles D. Morris
Center for Air Force C² Systems
email: cmorris@mitre.org
(781) 271-2443

Briefing Topics

- Background
- Utility Descriptions and Rational for Use
- Current Efforts and Status
- Questions

Background [1]

- **HQ USCENTCOM/J2SA has been working with Windows NT since 1994 in a mixed UNIX and NT environment**
- **J2SA developed “lock down” Utilities as a result of local ISSO’s “translation” of DIA/NSA requirements as they were first applied to an NT system in 1995**
- **The Utilities have been used operationally for 3 years (in NT v3.5, v3.51, and now NTv4.0)**

Background [2]

- The Utilities augment and/or repair Windows NT security and CM features
  - transparently to the user
  - with maximum flexibility for the administrator
- The Utilities were developed for the Top Secret/SCI environment, but have important applicability at all security levels

Utility Applications - Listing

- Clear Temporary Directory **on Logout**
- Event Backup **and Install Service for Security Audit Logs**
- Logout **on Security Log full Event**
- ProcessCheck **(and ProcessDll) to prevent unauthorized program use**
- FolderCheck **to complete NT's Hide Drive capability**
- UnixStart **to provide a single logon capability for X Server applications**
- Query Computer name **from Desktop**

Utility Descriptions and Rational for Use

- Clear Temp

Program: **Clear temp directory - clrtemp.exe**

Purpose: **Deletes all files in the temp directory identified by the TEMP environment variable when the user logs off.**

Rational: **This software directly addresses a Security SRS requirement to remove all temporary files which is not supported in either the NT3.51 or NTv4.0 software.**

Description: **The program is started by using a start command in the logon script. The program will wait until NT sends a WM_QUERYENDSESSION message, at which point all files in the temp directory are deleted**

Utility Descriptions and Rational for Use

- Event Backup

Program: **Event Backup Service**

Purpose: **Install and run the event backup service on a Domain Server so that every night at 1 am the service will copy the Security Event Logs from all Domain clients to the Domain Server and then clear them.**

Rational: **This software directly addresses Security SRS requirements on the maintenance and backup of security audit files that are not directly supported in either the NT3.51 or NTv4.0 software**

Description: **[see chapter 16 in the NT C&I Guide]**

Utility Descriptions and Rational for Use

- Logout on Full Audit Log event

Program: **logout.exe**

Purpose: **The logout program is designed to allow only the Administrator to log on if the Security Log is full or if the CrashOnAuditFail key is missing from the Registry.**

Rational: **This software directly addresses Security SRS requirements on the maintenance and backup of security audit files that are not directly supported in either the NT3.51 or NTv4.0 software.**

Description: **[see chapter 16 in the NT C&I Guide]**

Utility Descriptions and Rational for Use

- Process Check

Program: **processcheck.exe, dll**

Purpose: **Provides the System Administrator a mechanism to restrict the processes that a user can run.**

Rational: **This software directly addresses Security SRS requirements to limit or restrict user access to the shell and command line prompts, to control access to restricted programs, directories and files.**

These software modules extend existing Windows NT capabilities included as part of the NT policy editor, and correct NT OS behavior to allow it to conform or meet Security SRS requirements.

Description: **[see chapter 16 in the NT C&I Guide]**

Utility Descriptions and Rational for Use

- Folder Check

Program: **folderchek.exe**

Purpose: **Provide System Administrator a mechanism to prevent user access to restricted disk drives.**

Rational: **This software directly addresses Security SRS requirements to limit or restrict user access to the shell and command line prompts, to control access to restricted programs, directories and files.**

Foldercheck extends existing an Windows NT capability to “hide drives” included as part of the NT policy editor, and corrects NT behavior to allow it to conform or meet Security SRS requirements.

Description: **[see chapter 16 in the NT C&I Guide]**

Utility Descriptions and Rational for Use

- Unix Start

Program: **Unixstart.exe**

Purpose: **Provides a consistent and simplified UNIX application launch for all NT users. Establishes a mechanism for the system adminstrator to manage a “single logon” capability between UNIX and NT workstations. UNIX password and pass the information to the UNIX box for all X-applications.**

Rational: **This software provides significant simplification and administrative control over the mechanism used to launch UNIX application s for NT Workstations. All control is exercised through the administrator's setup and control of NT registry settings**

Utility Descriptions and Rational for Use

- Computer Name

Program: cmptrnm.exe

Purpose: **Provides a secure capability for the user to query the NT registry and identify the computer hostname**

Rational: **In many secure NT installations user access to the Control Panel applets is restricted. This can make it difficult for the user to determine the machine or host name assigned to the workstation or server. Service or help desk support can be delayed without this information being available.**

Description: **[see chapter 16 in the NT C&I Guide]**

Current Efforts and Status

- ESC DII AF Integration Facility has agreed to work with and sponsor the CENTCOM effort to segment the CSE-NT GOTS utility applications
- Application executables and source have been delivered to ESC DII AF
- Segment registration at DISA will be completed in Jan 98
- Segment design review will be in Early Feb 98
- Target is to include these utilities as a composite segment in the 3.3 build timeframe
- Rome Lab facilities are being investigated to augment
    - ESC testing
    - Documentation preparation
    - Software Distribution and CM support

NT GOTS Security Utilities
- Design Review Information Summary [1]

- **COE Compliance**
  - **Initially Level 5/6**
- **Functional Duplication**
  - **NONE**
- **External Software Requirements**
  - **NONE**
- **Software Licensing Issues**
  - **NONE**
- **Keyboard Mappings**
  - **NONE**
- **Color Mappings**
  - **NONE**
- **Standards Compliance**
  - **Fully I&RTS Compliant**
- **Architecture**
  - **SEE Utility Description Slides**
- **Segment Format**
  - **Software - Mission Applications**
- **Installation Process**
  - **Segment Install by Admin**
- **Network Discussion**
  - **Event Backup ?**
- **Approval Items**
  - **NONE**

NT GOTS Security Utilities - Design Review Information Summary [2]

- **Security Architecture**
  - **As per NT C&IG**
- **Segment Dependencies**
  - **NONE**
- **Resource Information**
  - **minimal**
- **Menu/Icon Additions**
  - **minimal**
- **Testing Requirements**
  - **NONE**
- **Documentation**
  - **SEE Follow-on Slide**

NT GOTS Security Utilities - Developer Documentation

Requirements

- Software Version Description (SVD)
- Installation Procedures (IP)
- Software Product Specification (SPS)
- Database Design Document (DBDD)
- System Administrator's Manual (SAM)
- Programmer's Manual (PM)
- Application Program Interface Reference Manual (APIRM)
- User's Manual (UM)
- Software Test Plan (STP)
- Software Test Description (STD)
- Software Test Report (STR)

DII COE SS Working Group

Windows NT GOTS Security Utilities

- *questions* -

Mr. Charles D. Morris
MITRE D510/DII AF
email: cmorris@mitre.org
(871) 271-2443